BTEC Assignment Brief

Qualification	Pearson BTEC Level 3 National Diploma in Engineering Pearson BTEC Level 3 National Diploma in Electrical/Electronic Engineering Pearson BTEC Level 3 National Diploma in Digital Engineering Pearson BTEC Level 3 National Extended Diploma in Engineering Pearson BTEC Level 3 National Extended Diploma in Electrical/Electronic Engineering Pearson BTEC Level 3 National Extended Diploma in Computer Engineering
Unit number and title	**Unit 38: Website Production to Control Devices**
Learning aim(s)	**A:** Investigate the technology used in website applications for controlling physical devices across the internet **B:** Investigate security measures used to protect website applications from malicious attacks
Assignment title	Investigating the server side technologies and security measures of web servers
Assessor	
Issue date	
Hand in deadline	
Vocational Scenario or Context	You have been employed as a Software Engineer at a small engineering organisation that specialises in SMART home appliances. The company is prototyping a Smart Technology-enabled fridge-freezer to challenge the larger companies in the market place. The company is targeting the high-end appliance market with its bespoke hardware and software solutions for the product. As an experienced software engineer, you have been assigned as lead developer for the web portal aspect of the project. You will need familiarise yourself with the technologies and languages in this area by researching similar website controlled devices on the market.
Task 1	You have been asked to investigate the technology used in website applications for controlling different devices, along with the security methods that are employed to protect website applications from malicious attacks. To do this: You will need to research the types of devices that can be controlled over the internet, and the methods that can be applied to protect website applications. You need to: • Research the types of device that can be controlled over the internet in each of the following areas: building management, visual devices, domestic appliances, industrial, health and wellness, inaccessible and dangerous applications. • Research the threats and vulnerabilities that can affect websites

	You then need to: Produce a report for at least three of the investigated devices and web application development environments. Your report should include: • Information about the type of device; • Information about the use of server-side scripting languages, including the language options that are available and issues around server requirements, scalability, documented support, cost, ease of use and security • Information about the structure of the application, including reference to login systems, authentication, file storage, data stores • A consideration of web server scripting, with reference to web application layout, database solutions, hosting and client-side requirements You should also consider the benefits and limitations of the use of server side scripting in each device. You should then: a) consider the effects of malicious threats and vulnerabilities on websites; b) the effects of malfunctions; and c) the security measures used to protect website applications. Your report should include: • Information about a range of malicious threats such as malware, eaves dropping, spamming, out of band; vulnerabilities from human error such as user error and weaknesses; and the consequences of hardware and software malfunctions. • An analysis of the measures to keep website applications protected and secure. You should include reference to security measures in server-side scripting, the use of Structured Query Language (SQL) and the impact of these security measures on the performance, usability and the overall effectiveness of the system.
Checklist of evidence required	A written report providing an introduction to scripting principles, covering security issues, and an introduction to scripting principles.

Criteria covered by this task:	
Unit/Criteria reference	To achieve the criteria you must show that you are able to:
38/AB.D1	Evaluate, using language that is technically correct and of a high standard, the effectiveness of the technologies and security protection measures used in the provision of a robust and secure website application.
38/A.M1	Compare the technologies used in website applications for the control of physical devices.
38/B.M2	Analyse the security threats to and vulnerabilities of website applications and the security protection measures available, including how these impact on performance and usability.
38/A.P1	Explain the technologies used in website applications for the control of physical devices
38/B.P2	Explain the security threats to and vulnerabilities of website applications and the security protection measures available.

Checklist of evidence required	A written report
Sources of information to support you with this Assignment	**Books** Pearson textbook specific to new BTEC Nationals in Engineering Donahoo, M., Speegle, G.; SQL: Practical Guide for Developers The Practical Guides; Elsevier, 2010; ISBN 9780080489742 **Websites** khanacademy.org - a collection of computer science and programming tutorials msdn.microsoft.com - The Microsoft Developer Network includes information on securing web servers digicert.com/ssl.htm - An SSL provider Above are some examples of websites. Further useful resources may be found at qualifications.pearson.com/en/support/published-resources.html#step1